

.....

Centrify Mobile Authentication Services

SDK Quick Start Guide

7 November 2013

Centrify Corporation



Legal notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrifry Corporation provides this document and the software described in this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrifry Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrifry Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrifry Corporation may make improvements in or changes to the software described in this document at any time.

© 2004–2013 Centrifry Corporation. All rights reserved. Portions of Centrifry DirectControl are derived from third party or open source software. Copyright and legal notices for these sources are listed separately in the Acknowledgements.txt file included with the software.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrifry, DirectAudit, DirectControl and DirectSecure are registered trademarks and DirectAuthorize and DirectManage are trademarks of Centrifry Corporation in the United States and other countries. Microsoft, Active Directory, Windows, Windows NT, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Centrifry Suite is protected by U.S. Patents 7,591,005, 8,024,360, and 8,321,523.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

Revision history

This table summarizes the changes that have been made to this document with each revision.

Date	Notes
11 September 2013	First draft.
24 September 2013	Added an introduction.

Contents

	Revision history	2
Chapter 1	Introduction	4
	Centrify SSO enhances the user’s experience and improves security	4
	Use the MAS API to add SSO to mobile applications	5
Chapter 2	Developing with the Centrify MAS API	7
	Contents of the MAS SDK package	7
	Prepare for development	8
	Install and configure the Centrify application	8
	Install and run the demo application	10
	Create a SAML application profile in Centrify Cloud Manager	11
	Use the sample project to write your application	11
	Prepare your application for use	12
	Contact us	12

Introduction

The Centrify mobile application provides single sign-on (SSO) services on Android and iOS mobile devices through Centrify Cloud Service and communication with an Active Directory infrastructure.

This single sign-on solution addresses password proliferation by providing users with a single sign-on while also giving organizations centralized control over access to web-based and mobile applications. Users not only enjoy single sign-on but also self-service features that let them locate, lock, or wipe their mobile devices and reset their Active Directory passwords. Centrify Cloud Service delivers access control and visibility to application use in addition to seamless integration with Microsoft Active Directory. Centrify Cloud Service single sign-on decreases the cost of rolling out and managing web-based and mobile applications while improving user adoption, satisfaction, security and productivity.

Centrify SSO enhances the user's experience and improves security

Employees of a large organization typically have to use several web-based and mobile applications on a daily basis, such as file-sharing applications, business-networking applications, email, and so forth. Whether they access the applications through a web browser or through applications on a mobile device, they normally have to provide a username and password for each application, each time they open the application. Because it's difficult to remember a large number of passwords, users often use one or a small set of passwords for all the applications they need to use. If one of those applications has a security vulnerability and a user's password is compromised, a malicious hacker might gain access to all of the employee's data in all of the applications that employee uses.

Centrify Cloud Service provides authentication using industry-standard certificate-based security and the organization's Active Directory service. For SaaS applications, the organization provides users with the MyCentrify portal through which they can access all the applications with which the organization has an account. The user logs in once with his or her Active Directory credentials to gain access to all the SaaS applications that use Security Assertion Markup Language (SAML) protocol to authenticate users. For mobile applications that use the Centrify API to get SSO through Centrify Cloud Service, a similar situation applies: once the user has registered the device with Centrify Cloud Service, he or she has access to every such SSO application on the device. Most such mobile applications have a web service providing data in the background, and the SSO extends to the web service without any additional credentials from the user.

Use the MAS API to add SSO to mobile applications

Mobile applications can use the Centrify Mobile Authentication Service (MAS) APIs to authenticate with Centrify Cloud Service.

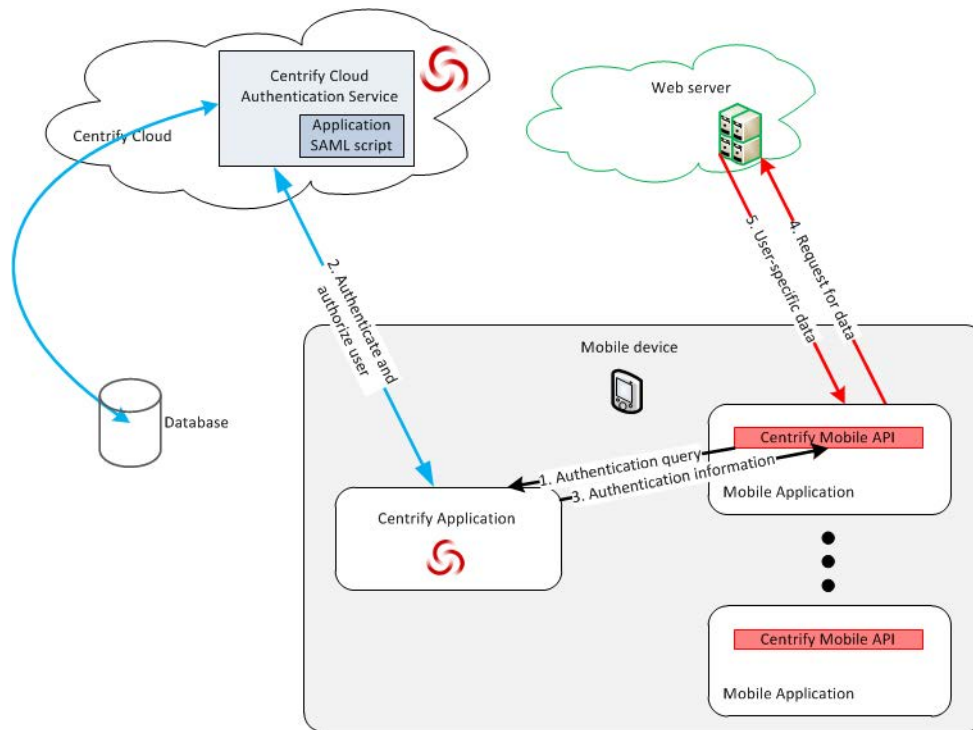
On an Android or iOS device, the user installs the Centrify application to obtain access to Centrify Cloud Service. The Centrify application establishes a certificate-based trust relationship with Centrify Cloud Service. The first time the user opens the Centrify application or any other application on the device uses the MAS API to authenticate the user, Centrify Cloud Service prompts the user for Active Directory credentials, authenticates the user of the device, validates that the user has a current Active Directory account, and looks up the user's roles to determine which applications the user is allowed to run. After that, whenever an application calls the MAS API, the Centrify application provides the user's authentication information. The Centrify application uses the trust relationship it has established with Centrify Cloud Service to get Active Directory and authentication information without any further interaction with the user. The user experience can be described as "zero sign-on" since, after initial enrollment, the user is never required to enter credentials.

Centrify Cloud Service and the Centrify MAS APIs use SAML to authenticate users. The authentication token returned by Centrify Cloud Service to the application is a SAML response. However, because the MAS APIs take care of validating and parsing the token, you do not need to know anything about SAML to implement SSO using the MAS APIs.

The MAS APIs provide general information about the user read by Centrify Cloud Service from the user's Active Directory entry, such as the login user name, the user's address and telephone number, and their email address. If you need other attributes from Active Directory, you can add them to the authentication token using an application-specific SAML script run by Centrify Cloud Service when the user first opens the mobile application. The script is created by the administrator when configuring the Generic SAML template in Centrify Cloud Manager for the application. See *Centrify Mobile Authentication Services SDK Implementation Guide* for instructions on using the Generic SAML template.

When the login sequence is initiated by the user opening a mobile application, the sequence of events is as shown in the following figure.

- • • • • Use the MAS API to add SSO to mobile applications



When the user installs and starts up a mobile application that uses the Centrify MAS API, Centrify Cloud Service requests Active Directory credentials from the user and uses them to authenticate and authorize the user. After that the device is recognized by Centrify Cloud Service.

- 1 The user opens the mobile application and the application requests authentication information using the MAS API.
- 2 This information might be cached, but if the cached information has expired, the Centrify application contacts Centrify Cloud Service to obtain it using the certificate-based trust relationship set up earlier. In either case, the process is invisible to the user.

Note In order for Centrify Cloud Service to generate an authentication token, an administrator must use Centrify Cloud Manager to create and configure an application-specific SAML application profile and script. See *Centrify Mobile Authentication Services SDK Implementation Guide* for instructions on configuring a SAML application profile.

- 3 The Centrify application returns the information, including the authentication token if requested, to the application.
- 4 The application passes the authentication token to its web service and requests resources for the user.
- 5 The application's web service uses the token to authenticate the user and returns the user's data for the application to display.

The user can now use the mobile application.

Developing with the Centrifly MAS API

This guide shows you how to quickly start development with the Centrifly Mobile Authentication Service (MAS) API to create a mobile application designed to run on an Android or iOS mobile device.

The Centrifly MAS API is specifically designed to provide single-sign-on (SSO) capabilities to applications running on an Android or iOS mobile device. The Centrifly application on the device authenticates the user through Centrifly Cloud Services and, after that, the user does not need to provide credentials in order to use any of the SSO applications.

Refer to *Centrifly Mobile Authentication Services SDK Implementation Guide* to understand the roles of the MAS API, Centrifly Cloud Service, the Centrifly application, other mobile applications, and SaaS applications.

Contents of the MAS SDK package

The Android MAS SDK is packaged in the `Android` folder in the `centrifly-cloud-SDK` zip file.

See the `ReadMe` file included in the `Android` folder for an up-to-date enumeration of the files in the SDK. As of the time of this writing, in addition to the `ReadMe` file, the SDK package contains three folders:

- `centriflyauth2-1.0-SNAPSHOT.jar`: The Centrifly MAS SDK library.
- `javadoc`: A folder containing Javadoc documentation for the API. *Centrifly Mobile Authentication Services SDK Implementation Guide* also has documentation for the API; see the chapter “Mobile Authentication Service Android Reference.”
- `samples`: A folder containing the following:
 - `GenericSSODemo1.apk`: A demo app.
 - `GenericSSODemo2.apk`: A demo app.
 - `GenericSSODemo1`: A folder containing source code for `GenericSSODemo1.apk`.

The iOS MAS SDK is packaged in the `iOS` folder in the `centrifly-cloud-SDK` zip file.

See the `ReadMe` file included in the `iOS` folder for an up-to-date enumeration of the files in the SDK. As of the time of this writing, in addition to the `ReadMe` file, the SDK package contains three folders:

- `libs`: The Centrifly MAS framework header files.

- **Doc:** A folder containing documentation for the API. *Centrify Mobile Authentication Services SDK Implementation Guide* also has documentation for the API; see the chapter “Mobile Authentication Service iOS Reference.”
- **Samples:** A folder containing source code and the Xcode project for the CentrifySDKSample sample app.

Prepare for development

- 1 Go to <https://www.centrify.com/cloud/cloud-service-registration.asp> and follow all the steps to register for Centrify Cloud Service and install the Centrify Cloud Proxy Server.

When you register, Centrify Cloud Service displays a window with a customer ID and proxy activation code. Make a note of the ID and copy the activation code to your clipboard.

- 2 Connect your production or test Active Directory environment to Centrify Cloud Service as instructed at <https://www.centrify.com/cloud/cloud-service-registration.asp>.
- 3 Open Cloud Manager at <https://cloud.centrify.com/manage>. You need the sdkdemo test application in Cloud Manager (necessary for the sample applications to work):
 - a Click **Add App**.
 - b Search for the sdkdemo application in the Select Applications dialog, select it and click **Add Apps**.
 - c Follow the directions in the online help to configure the application.

Install and configure the Centrify application

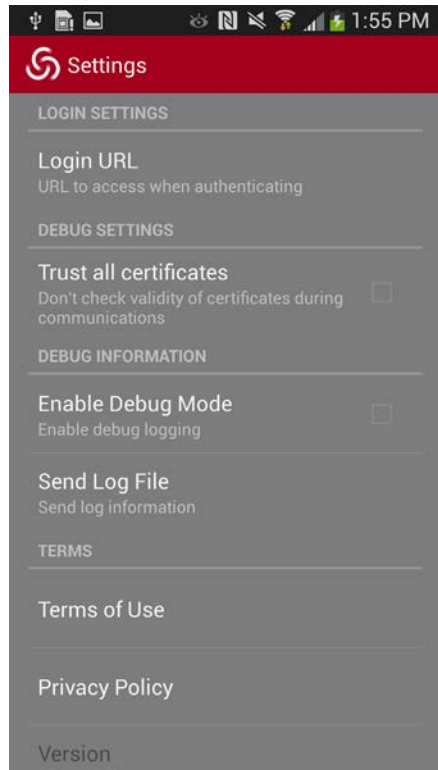
The Centrify application can be run on any mobile device running Android 2.3 or later or iOS 6 or later. The Centrify application must be version 13.10 or later.

- 1 Download the Centrify application from Google Play or the Apple App Store and install it on the mobile device.

- • • • • Install and configure the Centrify application

- 2 Launch the Centrify app and, under **Settings**, make sure the login URL is set to `https://cloud.centrify.com`. Click **Enable Debug Mode**.

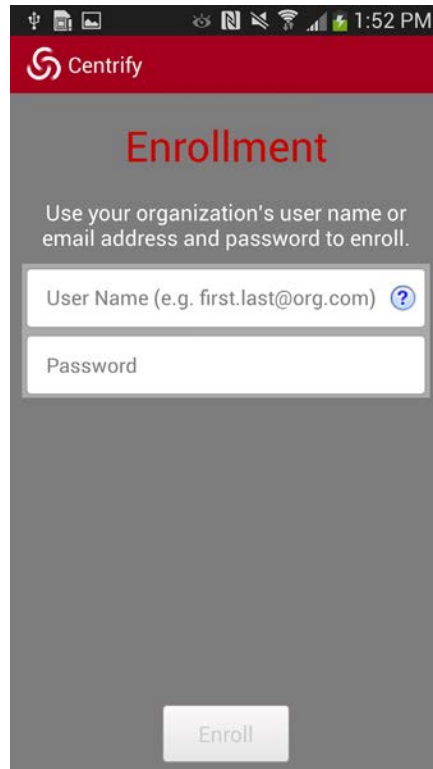
Figure 1. Centrify app settings



- • • • • Install and run the demo application

- 3 On the Enrollment screen, enter the Active Directory credentials for the user allowed to register the mobile device with Centrify Cloud Service.

Figure 2. Log in with Centrify app



Install and run the demo application

The demo applications can be tested on any mobile device running Android 2.3 or later or iOS 6 or later.

- 1 For Android, install the Generi cSS0Demo1. apk sample application on the Android device. For iOS, install the Centri fySDKSampl e sample app on the iOS device or use the emulator in Xcode.

Note Android program (apk) files can be installed on both devices and emulators using adb tools, which are part of the Android SDK. For more details, refer to <http://developer.android.com/sdk/index.html>.

For details on how to test an iOS app on a device, refer to <https://developer.apple.com/library/mac/documentation/IDEs/Conceptual/AppDistributionGuide/TestingYouriOSApp/TestingYouriOSApp.html>.

- 2 Launch the sample application.
- 3 Try the buttons in the sample application to see the information returned by Centrify Cloud Service.

- 4 Close the sample application and reopen it. You should not have to enter credentials again.

Create a SAML application profile in Centrify Cloud Manager

You need to add an application profile for your mobile application so that it will appear in the list of available applications in MyCentrify. In addition, you need to add a SAML application profile for your back-end SaaS application so that Centrify Cloud Services can generate the authentication token needed by the SAML interface.

- 1 Open Centrify Cloud Manager and click **Add App** on the **Apps** page.
- 2 Enter Android in the search field. Select the Android InHouse template, and click **Add App**.
- 3 Click **Edit** and enter a name, description, and icon for your mobile application. Click **Save**.
- 4 Click **Add App** and enter Generic in the search field. Select the Generic SAML template and click **Add App**.
- 5 Follow the online help instructions and the instructions in the chapter “Creating a SAML application profile” of the *Centrify Mobile Authentication Services SDK Implementation Guide* to fill in the template for the back-end web service that works with your mobile application.

Use the sample project to write your application

- 1 Open the source code for the sample application (Generi cSS0Demo1 for Android, Centri fySDKSampl e for iOS).
- 2 Find the getSecuri tyToken call in the file Sal esRecordsActi vi ty. j ava. This method retrieves the authentication token for the application. For example:

```
try {
    String target = Preferences.getTarget(Sal esRecordsActi vi ty. thi s)
    saml Token = Enterpri seAuthenti cati on. getSecuri tyToken(target, fal se,
        Sal esRecordsActi vi ty. thi s)
    if (saml Token == null || saml Token. length() == 0) {
        Toast. makeText(Sal esRecordsActi vi ty. thi s,
            "No saml token found", Toast. LENGTH_ SHORT). show();
        return null;
    }

    publi shProgress("Auth token obtai ned. . .");
}
```

In the sample application, the application name (target) passed to the getSecuri tyToken method is "sdkdemo", as defined in the file Preferences. j ava. This call will work only if you have an application named sdkdemo in Centrify Cloud Manager

created using the Generic SAML template. Centrify Cloud Services uses the SAML script specified in the Generic SAML template to generate the token.

For iOS, find the `getSecurityTokenForTarget:` call in the files `AppDelegate.m` and `HomeViewController.m`. This method retrieves the authentication token for the application. For example:

```
- (IBAction)getAccessToken: (id)sender
{
    self.accessToken = nil;
    [EnterpriseAuthentication getSecurityTokenForTarget:@"sdksdemo"
    alwaysUseFreshToken:NO completionHandler:^(CentrifySDKResult *result) {
        [self getSecurityTokenHandler:result];
    }];
}
```

Notice that, in the sample application, the application name passed to the `getSecurityToken` or `getSecurityTokenForTarget:` method is "sdksdemo". This call will work only if you have an application named sdksdemo in Centrify Cloud Manager created using the Generic SAML template. Centrify Cloud Services uses the SAML script specified in the Generic SAML template to generate the token.

- 3 Write your application using the Centrify MAS API to authenticate the user and parse the authentication token. Be sure that your call to `getSecurityToken` or `getSecurityTokenForTarget:` uses the same application name as you used in your Generic SAML template for your web service.

Note You will need to get some parameter values for the methods in the API from Cloud Manager. See the API descriptions in the chapter “Mobile Authentication Service Android Reference” or “Mobile Authentication Service iOS Reference” for details.

Prepare your application for use

- 1 Test your mobile application for SSO.
- 2 Submit your compiled and tested mobile application to Centrify at devsupport@centrify.com.
- 3 Provide the following information to Centrify so that Centrify can perform quality assurance testing and can include the application in the Centrify Application catalog:
 - Any configuration of the SAML template in Cloud Manager needed to support your SAML interface; for example, the contents of the **URL** and **Issuer URL** fields and the script from the **Advanced** tab.
 - At least one test account credential for the service that you have enabled for SSO.

Contact us

If you have any questions, comments, or feedback, please email us at devsupport@centrify.com.